DOD Privacy Impact Assessment (PIA)

1. DA organizational name (APMS Sub Organization name).

U.S. Army, Office of the Assistant G-1 for Civilian Personnel

2. Name of Information Technology (IT) System.

Fully Automated System for Classification Production system (FASCLASS Prod)

3. Budget System Identification Number (SNAP-IT Initiative Number).

9990

4. System Identification Numbers(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

2984

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable).

N/A

6. Privacy Act System of Records Notice Identifier (if applicable).

A0690-200 DAPE, Department of the Army Civilian Personnel Systems

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

N/A

8. Type of authority to collect information (statutory or otherwise).

5 U.S.C. 301, Departmental Regulations
5 U.S.C. 51
10 U.S.C. 3013, Secretary of the Army
Army Regulation 690-200, General Personnel Provisions
Executive Order 9397

9. Provide a brief summary or overview of the IT system (activity/purpose, present lifecycle phase, system owner, system boundaries and interconnections, location of the system and components, and system backup)

FASCLASS is a web-based centralized classification system that was developed to completely automate position description master files and organizational records by

converting manual data and existing systems into a standard electronic form. A position description library functionality is also incorporated into FASCLASS. FASCLASS is an existing system that in the operation and maintenance life cycle phase. The system contains information pertaining to Army civilian workforce personnel. The Army Civilian Personnel Network (ACPNet) is connected to the DoD Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) via the installation backbone. PC-to-server and server-to-server connections are protected by encryption tools. Data transferred is also protected by encryption. Site-to-site connections are protected by a Virtual Private Network. FASCLASS interfaces with the Defense Civilian Personnel Data System (DCPDS) through a secured server. Users can access the system via a web browser. Web servers and application servers are located in Alexandria, VA. The database servers are located in Rock Island, Illinois. The FASCLASS system is backed up daily via tape backups. Tapes are maintained up to six months at the Army Civilian Data Center.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g. names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.)

Information in identifiable form that is collected includes: name, social security number, date of birth, national identifier, pay grade, the servicing Civilian Personnel Advisory Center (CPAC), sequence number, occupational code, personnel office identifier information, and employment title. Information used by FASCLASS is extracted from DCPDS through a secure server via an encrypted network.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

Information used by FASCLASS is extracted from DCPDS through a secure server via an encrypted network.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.).

FASCLASS was developed to completely automate civilian position description master files and organizational records. The Office of the Assistant G-1 for Civilian Personnel was established under the Secretary of the Army to carry out these mandates. Information in identifiable form is collected and used by this system in direct support of these missions.

13. Describe how the information in identifiable form will be used (e.g. to verify exiting data, etc.).

Information in identifiable form will be matched and combined with appropriate position descriptions. It is also used to verify whether users are authorized to set up an account with the FASCLASS system.

14. Describe whether the system derives or creates new data about individuals through aggregation.

This system does not derive or create new information about individuals through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

Information will be available to authorized users with a need to know in order to perform official government duties. Information from this system is shared among the Army personnel community which consists of the Civilian Personnel Operations Centers, the Civilian Personnel Advisory Centers, Army Civilian Human Resources Agencies and U.S. Army Garrisons at installations and Headquarters, U.S. Army Installation Management Command. Commanders and supervisors of civilian personnel are also provided information from the system. Internal DoD agencies that would obtain access to Personally Identifiable Information in this system, on request in support of an authorized investigation or audit, may include Department of Defense Inspector General, Defense Manpower Data Center, Defense Criminal Investigative Service, Defense Information Systems Agency, Defense Contract Management Agency, Under Secretary of Defense for Personnel & Readiness, Army Staff Principals in the chain of command, Department of Army Inspector General, Army Audit Agency, US Army Criminal Investigative Command, US Army Intelligence and Security Command, Provost Marshal General and Assistant Secretary of the Army for Financial Management and Comptroller. In addition, the DoD blanket routine uses apply to this system.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to contest to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

Information used by FASCLASS is extracted from DCPDS through a secure server via an encrypted network. Individuals are not involved in this data collection process. Individuals are furnished privacy advisories when initially employed by the Department of Army and are implicitly consenting to the capture and use of this information.

17. Describe any information that is provided to and individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of the delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

Information in identifiable form is not collected directly from the individual thus they are not provided a Privacy Act Statement or Privacy Advisory upon collection by this system.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

This system has a current certification and accreditation. The system resides on a secure military installation within secure facilities. These facilities have armed guards that verify the credentials (appropriate DoD building/identification badge) of all employees and login all visitors including, vendors and maintenance. Cameras are also used to monitor activity around the installation. Additionally, the system is built on redundancy with a full COOP site. System users include Army Civilian and contract Personnel under the administrative control of the Chief Information Services Division (CISD). Personnel with system administration privileges are required to have background investigations at the ADP/IT I or II level and to sign a non-disclosure statement. All personnel accessing government computer information are required to have a minimum of automatic data processing / information technology (ADP/IT) level III background investigation.

Users may have access requirements and are limited to specific or general information in the computing environment. The system administrator defines specific access requirements dependent upon each user's role. Each specific application in the system may further restrict access via application-unique permission controls. Users must enter appropriate user/Identification and password before being authorized access to the resources. A user's manual was designed to fulfill the needs of the different types of employees (e.g., users, administrators, managers, etc.). Additionally, all aspects of privacy, security, configuration, operations, data retention and disposal are documented to ensure privacy and security are consistently enforced and maintained. There is routine monitoring of security events, network intrusion detection, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIGs). Files transferred across the internet/NIPRNET are encrypted.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program" November 11, 2004. If so, and a System of Records Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when the publication of the notice will occur.

This system requires a SORN and it is published.

20. Describe/evaluate any potential privacy risk regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate and privacy risks in providing individuals and opportunity to object/contest or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Safeguards are employed to detect and minimize unauthorized disclosure, modification, and/or destruction of data; thus we believe the risk to the individual's privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Risks are further mitigated by the implementation of firewalls, intrusion detection systems and malicious code protection

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

The data in the system is For Official Use Only. The PIA may be published in full.